USAISEC
US Army Information Systems Engineering Command
Fort Huachuca, AZ 85613-5300

(2)

U.S. ARMY INSTITUTE FOR RESEARCH
IN MANAGEMENT INFORMATION,
COMMUNICATIONS, AND COMPUTER SCIENCES

AIRMICS

FAISS Access to DODIIS Alternatives

ASQB-GM-91-012

January 1991

AIRMICS
115 O'Keefe Building
Georgia Institute of Technology
Atlanta, GA 30332-0800

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188
Exp. Date: Jun 30, 1986

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS NONE
2a. SECURITY CLASSIFICATION AUTHORITY N/A	3. DISTRIBUTION/AVAILABILITY OF REPORT N/A
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) ASQB-GM-91-012	5. MONITORING ORGANIZATION REPORT NUMBER(S) N/A
6a. NAME OF PERFORMING ORGANIZATION AIRMICS 6b. OFFICE SYMBOL (*If applicable*) ASQB-GM	7a. NAME OF MONITORING ORGANIZATION N/A
6c. ADDRESS (City, State, and Zip Code) 115 O'Keefe Bldg. Georgia Institute of Technology Atlanta, Ga 30332-0800	7b. ADDRESS (*City, State, and ZIP Code*) N/A
8b. NAME OF FUNDING/SPONSORING ORGANIZATION AIRMICS 8b. OFFICE SYMBOL (*If applicable*) ASQB-GM	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (*City, State, and ZIP Code*) 115 O'Keefe Bldg. Georgia Institute of Technology Atlanta, GA 30332-0800	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. 62783A; PROJECT NO. DY10; TASK NO. 05; WORK UNIT ACCESSION NO.
11. TITLE (*Include Security Classification*) FAISS Access to DODIIS Alternatives	
12. PERSONAL AUTHOR(S) John Wandelt	
13a. TYPE OF REPORT	13b. TIME COVERED FROM_____ TO_____
14. DATE OF REPORT (*Year, Month, Day*) January 1991	15. PAGE COUNT 25
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES			18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*)

This document provides a brief overview of alternatives for providing FORSCOM Automatic Intelligence Support System (FASISS) connectivity to the Department of Defense Intelligence Information System (DODIIS). The Defense Secure Network III (DSNET3) is the sensitive Compartment Information (SCI) system high portion of the Defense Data Network (DDN) which provides Wide Area Network (WAN) backbone connectivity to the Department of Defense (DOD) intelligence community. Connectivity to DSNET3 will provide FAISS subscribers with a means of accessing remote Defense Intelligence Agency (DIA) databases as well as providing a channel for data transferral between geographically dispersed FAISS users. The alternative configurations described in this document are all based on connectivity to DSNET3 via a communications link to a DSNET3 Packet Switched Node (PSN). Alternatives which require connection to DSNET3 via already existing minicomputer or mainframe host are not considered in this document.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Michael Evans	22b. TELEPHONE (*Include Area Code*) (404) 894-3107 22c. OFFICE SYMBOL ASQB-GM

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

This research was performed for the Army Institute for Research in Management Information, Communications and Computer Science (AIRMICS), the RDTE organization of the U.S. Army Information Systems Engineering Command (USAISEC). This research is not to be construed as an official Army position, unless so designated by other authorized documents. Material included herein is approved for public release, distribution unlimited. Not protected by copyright laws.

THIS REPORT HAS BEEN REVIEWED AND IS APPROVED

s/ James Gantt
James Gantt
Chief, MISD

s/ John R. Mitchell
John R. Mitchell
Director
AIRMICS

DOCUMENT CONTROL NUMBER: A-8752-106

January 15, 1991

FAISS ACCESS TO DODIIS ALTERNATIVES

Contract No. DAFK11-86-D-15-0030

Prepared for:

DEPARTMENT OF THE ARMY

Headquarters, Forces Command

Ft. McPherson, Georgia 30330-6000

Prepared by:

John Wandelt

Computer Science and Information Technology Laboratory

Georgia Tech Research Institute

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

FAISS ACCESS TO DODIIS ALTERNATIVES
DCN: A-8752-106; January 15, 1991

1. PURPOSE.

This document provides a brief overview of alternatives for providing FORSCOM Automated Intelligence Support System (FAISS) connectivity to the Department of Defense Intelligence Information System (DODIIS). The Defense Secure Network III (DSNET3) is the Sensitive Compartment Information (SCI) system high portion of the Defense Data Network (DDN) which provides Wide Area Network (WAN) backbone connectivity to the Department of Defense (DOD) intelligence community. Connectivity to DSNET3 will provide FAISS subscribers with a means of accessing remote Defense Intelligence Agency (DIA) databases as well as providing a channel for data transferral between geographically dispersed FAISS users. The alternative configurations described in this document are all based on connectivity to DSNET3 via a communications link to a DSNET3 Packet Switched Node (PSN). Alternatives which require connection to DSNET3 via an already existing minicomputer or mainframe host are not considered in this document.

This document does not intend to be an exhaustive list of all possible configurations, neither does it purport to describe any alternative in sufficient detail for implementation. This document does describe an initial set of alternatives in sufficient detail to aid in formulating a short, intermediate, and long term solution for FAISS connectivity.

A section titled 'Technical Unknowns' accompanies each alternative configuration. The purpose of this section is to present an initial set of unknowns which must be resolved prior to pursuing the corresponding alternative as the base configuration. It should be understood that the inability to resolve a technical unknown may signify that the described alternative is neither implementable nor desirable.

Section 2 of this document describes the standard protocol architecture of the DDN. The implementation of any alternative which utilizes the DDN as a WAN backbone must ensure conformance to the DOD implemented protocol suite. This section is included for completeness only and may be quickly skimmed; alternative configurations are described starting in Section 3.

2. PROTOCOL ARCHITECTURE

The protocol architecture for the proposed alternatives is based on the standard DOD protocol suite. This is currently implemented on the Defense Data Network (DDN) and described in the DDN Protocol Handbook compiled by the DDN Network Information Center (NIC) for the Defense Communications Agency (DCA). The official internet protocol architecture is also identified in Request For Ccomments (RFC) 1140, Defense Advanced Research Projects Agency, Internet Activities Board: "IAB official Protocols".

Although it is necessary to adhere to the DOD protocol suite for communications across the DSNET, it is possible to utilize additional protocols, such as Novell's Sequence Packet eXchange (SPX) and Internet Packet eXchange (IPX), for communications on the local network. However, such a multi-protocol approach may add to the complexity and cost of the implementation.

It is expected that due to the governments acceptance of the Government Open System Interconnection (OSI) Profile (GOSIP) the DDN (thus DSNET3) will develop a plan to support GOSIP specified protocols. This plan will most likely provide support for both the TCP/IP and GOSIP protocol suites for a specified time period (perhaps indefinitely). Dual protocol stacks and Applications Level Gateways (ALG) will probably be utilized to provide transparency to subscribers. Until the DDN supports the GOSIP protocols, connectivity will be based on the TCP/IP protocol suite.

2.1 APPLICATION AND SERVER PROTOCOLS.

2.1.1 File Transfer

File transfers will be performed using the DOD File Transfer Protocol (FTP). FTP will be implemented in accordance with MIL-STD 1780 and RFC 959. The minimum implementation described in RFC 1123, "Requirements for Internet Hosts -- Application and Support," shall be supported. The FTP implementation will be able to transmit both ASCII text and binary files. The FTP implementation shall provide both FTP client and server capability. When implemented on a single tasking platform (i.e. MSDOS) it is not necessary for the FTP server portion to run as a background process, although this is still possible and desirable.

2.1.2 Virtual Terminal

Virtual terminal support will be provided with the TELNET protocol. The TELNET protocol will be implemented in accordance with MIL-STD 1782 and RFC 854. The following TELNET options will be implemented: TELNET Binary Transmission (RFC 856), TELNET Echo (RFC 852), TELNET Suppress Go Ahead (RFC 858). The following options are not necessary but desirable: TELNET Status (RFC 859), TELNET Timing Mark (RFC 860), TELNET Extended Options List (RFC 861), TELNET End of Record (RFC 885), and TELNET Terminal Type (930).

2.1.1.1 Telnet Application

The Telnet application shall provide terminal emulation to the following standard DEC terminals: VT52, VT100, VT220. In addition a standard ANSI terminal shall be supported. If the Telnet application does not directly support all of the above emulations it is sufficient to provide hooks (i.e. via interupt vector 14) to third party vendor packages which do provide the additional emulation capabilities. It is not necessary for the Telnet implementation on a single tasking platform (i.e. MS-DOS) to provide a Telnet server capability.

2.1.1.2 Network Virtual Data Entry Terminal (NVDET)

The NVDET application provides support for those host applications which require terminals which better facilitate data entry functions than standard scroll-mode

Teletype terminals. NVDET provides mechanisms for specifying on-screen fields with special attributes. NVDET will be implemented in accordance with RFC 1043, "Telnet Data Entry Terminal Option:DODIIS implementation."

2.1.1.3 Telnet 3270 (TN3270) Application

The TN3270 implementation shall allow a FAISS workstation to be used as a 3270 terminal on an IBM host computer running the TELNET protocol. Full compliance with 3270 message format and functionality will be implemented. Both formatted and unformatted screens will be supported.

2.1.3 Electronic Mail

The mail transfer protocol shall be implemented as described in MIL-STD 1781 and RFC 821, "Simple Mail Transfer Protocol" (SMTP). The text message format shall be implemented as described in RFC 822, "Standard for the Format of ARPA Internet Text Messages." In addition, the SMTP implementation shall support mail exchange (MX) records, as described in RFC 974, "Mail Routing and the Domain System."

2.1.4 Distributed File System

Several distributed file system protocols are in existence. Although no directed specification for use on the Internet exists, the most widely implemented is the Network File System (NFS). If NFS is selected, it will be implemented as specified in RFC 1094, "NFS: Network File Protocol." External Data Representation (XDR) as described in RFC 1014 and Remote Procedure Call (RPC) as described in RFC 1057 shall also be implemented. These protocols, developed by SUN Microsystems Inc., work together to provide transparent, remote file access of file system resources in a heterogeneous environment of machines, operating systems, and networks.

2.2 TRANSPORT LAYER PROTOCOLS

A reliable end-to-end connection-oriented transport service shall be provide by the Transmission Control Protocol (TCP). TCP shall be implemented in accordance with MIL-STD 1778 and RFC 793. TCP port assignments shall be consistent with those specified in RFC 1117, "Internet Numbers", or its successor.

Connectionless transport service shall be provided by the User Datagram

Protocol (UDP). UDP shall be implemented as described in RFC 768.

2.3 NETWORK LAYER PROTOCOLS

A best effort Connection-less datagram service shall be provided by the Internet Protocol (IP). The IP shall be implemented in accordance with MIL-STD 1777 and RFC 791 as amended by RFC 950 "IP Subnet Extension", RFC 919 "IP Broadcast Datagrams", and RFC 922 "IP Broadcast Datagrams with Subnets." The IP implementation shall be able to process datagrams of at least 576 bytes. The following IP options will need to be implemented: security as described in RFC 1038, "Revised IP Security Option," loose source route, and strict source route. Although it is not necessary for the implementation to perform access control based on the security labels, the integrity of the Revised IP Security Option (RIPSO) fields should be maintained. Route record and the IP timestamp are desirable options.

The internet control message protocol (ICMP) will be implemented as described in RFC 792, "The Internet Control Message Protocol". Implementations should be capable of responding to all documented ICMP messages. The implementation should be capable of generating the ICMP message types: Echo Reply, Time Exceeded, and Parameter Problem. Gateway implementations shall be capable of sending the ICMP messages: Source Quench, Destination Unreachable, and ICMP Redirect.

Internet-to-MAC (media access control) address translation shall be implemented according to RFC 826, "An Ethernet Address Resolution Protocol." The ability shall exist to selectively disable address translation if necessary for local security.

2.4 DATA LINK AND PHYSICAL LAYER PROTOCOLS

At a minimum the data link and physical layer protocols must be able to support the network layer protocols described under Section 2.3. It is strongly recommended that the data link and physical layer protocols are implemented as specified by IEEE 802.2 and IEEE 802.3 (10base2, 10base5, and 10baseT) standards. Deviating from these standards in order to support fiber optic transmission medium for security reasons appears to be a valid justification. However, proprietary interfacing implementations

may limit availability of higher level protocol support.

2.5 NETWORK MANAGEMENT PROTOCOLS.

Although not mandatory, it is highly desirable to provide for integrated network management support. Integrated network management will provide the hooks necessary to allow the entire network to be managed as a single entity from a centralized location. The Simple Network Management Protocol (SNMP) as described in RFC 1157 is the recommended protocol for passing management information between managed objects and network management stations across the Internet. Compliance with the Structure of Management Information (SMI) as described in RFC 1155 and support of the Management Information Base (MIB) as specified in RFC 1156 are also necessary to provide manageability.

3. ALTERNATIVE #1

This alternative consists of a single F486 workstation which would be attached to a DIA accredited TCP/IP gateway. The gateway would be connected via an encrypted communications link (satellite, leased telco line, etc.) to a Packet Switched Node (PSN) on DSNET3. The F486 workstation would appear as any other host on DSNET3 and would be addressed with a unique IP address.

3.1 REQUIRED HARDWARE

The following hardware components are required to implement this alternative:

- F486 workstation
- DIA accredited ethernet TCP/IP gateway
- Fiber optic cabling (62.5 micron)
- Encrypted communications link

3.2 REQUIRED SOFTWARE

The following software components are required to implement this alternative:

- FAISS Verson 2.1 software
- Security Guardian
- Excelan TCP/IP LAN Workplace for DOS
- TN3270 for DOS
- NVDET for DOS

3.3 SECURITY FEATURES

The system security features will be provided by Security Guardian software, or an equivalent, commercial off the shelf package. The following security features will be provided:

- System logon via unique passwords

- Audit trails

- Menu control based on logon accounts

- Restriction from hard disk after floppy boot

- Allow discretionary access to files and directories

- Isolate users from DOS

3.4 ACCREDITATION ISSUES

The stand alone F486 workstation protected with Security Guardian software is technically equivalent, in terms of security risk, to a MITRE LAD node configured in stand alone mode. The Security Guardian security software provides equivalent security mechanisms as LANGARD or Watchdog security packages. As identified in the MITRE LAD Evaluation document, there are certain security holes which any software security package utilized in a directly connected mode is subject to. For example, it would be possible for the workstation to be booted from floppy and execute networking software from either the floppy or RAM drive to access the gateway and thus the PSN. This type of access would be possible without restriction or audit of *any* software based security package designed to run on the workstation. Additional non-auditable security related events such as multiple connections established from inside a network application are possible. Only the first connection is often registered by the security software as an audit entry.

It is believed that the previously mentioned issues will not present a restricting security risk if procedural and environmental security mechanisms in accordance with DIAM 50-4 are adopted in addition to the system security. Implementation of procedural security mechanisms should be fairly simple with a single machine configuration.

3.5 FUNCTIONALITY

Core functionality for this alternative includes:

- Menu control of system functions

- Remote file transfer (FTP)

- Remote virtual terminal (Telnet,TN3270,NVDET)

- Access to DODIIS mail via a host with mail capability

3.6 ADVANTAGES

The primary advantage of this alternative is that is relatively simple and straight forward to implement. Additionally, minimal administration is required to keep the system up and running.

3.7 DISADVANTAGES.

Since this alternative is based on a stand alone workstation, there is no local area network functionality built in. The following features will *not* be supported:

- Local mail capability

- Resource sharing (i.e. Gateway, disks, printers)

- Network data transfer between F486 workstations

This alternative does not preclude the existence of an independent LAN which provides some of this missing functionality. Floppy transfers between the stand alone workstation and the LAN would always be a possibility.

3.8 TECHNICAL UNKNOWNS

There are generally no technical unknowns. GTRI has successfully been able to connect the F486 to a TCP/IP based LAN using FiberComm fiber optic ethernet cards and Excelan's TCP/IP LAN Workplace for DOS commercial software package. Connection through the DIA accredited DSNET3 TCP/IP gateway located in the Sensitive Compartmented Information Facilty (SCIF) at the FORSCOM Command and Control facility has also been successfully demonstrated.

4. ALTERNATIVE #2

This alternative is identical to alternative #1 with the exception that multiple F486 workstations are connected to the gateway via a fiber optic ethernet. In this configuration, each workstation would have to be assigned a unique IP address which was known to the DSNET3 PSN's.

4.1 REQUIRED HARDWARE

The following hardware components are required to implement this alternative:

- F486 workstation(s)
- DIA accredited ethernet TCP/IP gateway
- Fiber optic cabling (62.5 micron)
- Encrypted communications link

4.2 REQUIRED SOFTWARE

The following software components are required to implement this alternative:

- FAISS Version 2.1 software
- Security Guardian
- Excelan TCP/IP LAN Workplace for DOS
- TN3270 for DOS
- NVDET for DOS

4.3 SECURITY FEATURES.

The security features for this alternative would be identical to the features provided in Alternative #1.

4.4 ACCREDITATION ISSUES

The accreditation issues specified for Alternative #1 also apply for Alternative #2. Due to the potential multiple points of intrusion, this alternative is slightly harder to secure and administer. Procedural security mechanisms must be enforced for all connected workstations. Additionally, it would be necessary to track multiple audit trails due to the fact that each workstation would only maintain a audit trail of events initiated from that workstation.

4.5 FUNCTIONALITY

In addition to the functionality described for Alternative #1, local network file transfer between any two local F486s will be supported. The implementation of this function will require both participating F486s to take an action to accomplish the file transfer. Specifically, one of the workstations will be put into server mode and the other will need to initiate a client request.

4.6 ADVANTAGES

An advantage of this alternative is that multiple F486 workstations are able to simultaneously share access to the DSNET3 gateway.

4.7 DISADVANTAGES

Although administration of this configuration is fairly straightforward, there are no provisions for centralized administration. The configuration of each F486 must be accomplished from its console. Additionally, this configuration would require multiple internet addresses (i.e. IP addresses) be obtained from the Defense Communications Agency (DCA).

4.8 TECHNICAL UNKNOWNS

Same as Alternative #1.

5. ALTERNATIVE #3

This alternative describes an implementation which provides enhancements to the security architecture of the first two alternatives. This alternative implements either a smart gateway or communications security server which is responsible for ensuring that all incoming and outgoing external connections are authorized, authenticated, and audited.

As described in Alternative #1, a DIA approved gateway is utilized to route traffic between the local LAN and a DSNET3 packet switched node. This gateway assumes that it should route all IP datagram traffic regardless of the generating source. Thus, the possibility of routing unauthorized traffic through DSNET3 is possible in some configurations. The gateway expects that local hosts only send traffic that is authorized, audited, and authenticated. This is typically enforced by mainframe or minicomputers which reside between the terminals/workstations and the gateway.

There are several approaches to providing the same level of security on a workstation based LAN. Consider the following:

a. Utilize a smart gateway which is capable of implementing authentication and auditing.

b. Place an independent communications security server between the gateway and the LAN segment which connects the local workstations. All external connections must pass through the communications security server.

c. Place the communications security server, gateway, and user workstations all on the same LAN segment. Configure the gateway so that it will only forward IP datagrams with a source or destination address equal to that of the communications security server. This forces all external connections to be passed through the communications security server. It will be necessary to make sure that a user workstation could not trick the gateway by modifying its address to match that of the communications security server.

d. Place a communications security server, gateway, and user workstations all on the same LAN segment. Configure the communications security server so that it monitors traffic between source and destination pairs; authorized traffic

will be logged while non-authorized traffic will be eliminated.

In each of the approaches described above it would be necessary to physically secure access to both the gateway and the communications security server.

The design of the MITRE LAD was centered around a Novell server architecture. One of the basic problems with the MITRE configuration was that the Novell server was not utilized as a communications security server to the DSNET3 gateway. All connections between the DSNET3 gateway and local workstations or between any two local workstations were accomplished without the participation or awareness of the Novell server. For a system without strict security requirements this design is desirable for performance reasons. However, the security requirements for this level of connectivity dictate tighter security measures at the cost of performance.

The remainder of this alternative will be described in terms of an implementation which utilizes a Unix communications security server. It should be understood that this alternative need not be restricted to a Unix implementation.

A Unix box with the proper software could be configured as communications security server which physically resides between the DSNET3 gateway and the LAN segment which attaches the FAISS workstations. The TCP/IP implementation must provide the ability to disable the automatic forwarding of IP datagrams between the two interfaces. This would force workstation users to first logon to the Unix box via a local telnet session prior to establishing a remote connection through the gateway. This two step connection process would shield the gateway attached to the DSNET3 PSN from direct access by the user workstations. Access to the gateway is effectively controlled by password access to the Unix box. A centralized external communications audit trail could also be maintained. By physically isolating and securing the Unix box from the user workstations this security architecture provides similar security mechanisms to that of existing connected systems.

5.1 REQUIRED HARDWARE

The hardware necessary to support this alternative would be the same as Alternative #2 plus any additional hardware to support the communications security server. The hardware necessary to support the communications security server depends on the method implemented as well as product availability. Further investigation and

prototyping are necessary to determine a specific hardware listing.

5.2 REQUIRED SOFTWARE

The software required for this alternative must also be determined by further investigation and prototyping.

5.3 SECURITY FEATURES

The enhanced authorization, authentication, and auditing of external communications provided by the addition of a communication security server into the LAN should make accreditation easier to attain. This security architecture provides multiple layers for securing and tracking external communications. First, each workstation is configured with a local security package such as LANGARD or Watchdog as specified in Alternatives #1 and #2. Second, an intruder who gains access via the floppy drive will be monitored and stopped by the communications security server.

5.4 ACCREDITATION ISSUES

The possibility of a workstation booting from a floppy and attempting to bypass the communications security server still exists. It is assumed that the communications security server is capable of detecting, countering, and logging such attempts. This differs from the prior alternatives in that DSNET3 gateway, as configured, is not intelligent enough to enforce a security access policy for communications to and from the DSNET3 packet switched node.

5.5 FUNCTIONALITY

The functionality of this configuration from the users perspective is identical to Alternative #2. Increased security is the emphasis.

5.6 ADVANTAGES

The primary advantage of this alternative over that of Alternative #2 is that of enhanced security with regards to external communications.

5.7 DISADVANTAGES

The major disadvantage of this alternative is that the communications security server will require an individual capable of performing the required administration functions. Since the functionality of the security server is fairly limited, it is not anticipated that a significant amount of time or knowledge would be required to perform any of the necessary tasks. As always, it will be desirable to maximize the automation and centralization of such tasks.

Additionally, the communications security server may require an extra physical box to be fielded. This is not a significant disadvantage for a stationary LAN which is free of space restrictions and consists of several workstations. However, space restrictions imposed by anticipated fielding requirements of the LAN may be significant. Additionally, when there are only a few workstations per LAN, the cost of the communications security server per configuration may be significant. It is extremely desirable to have the communications security server functions performed by either the existing gateway or a box which also provides other servers. The next alternative will identify some of these services.

5.8 TECHNICAL UNKNOWNS.

The technical unknowns center around the availability of a communications security server and the tradeoffs based on the method utilized:

a. Is it possible to configure/program the DSNET 3 gateway so that it can perform as a security server?

b. Can a general purpose Unix box be configured as a security server? Can IP forwarding between multiple interfaces be disabled? Will secure versions of Unix and TCP/IP (i.e. AT&T System V/MLS and TCP/MLS) provide mechanisms to allow this functionality?

c. Should a multi-level secure network product such as VSLAN from Verdix Corp be utilized as the communications sentry?

It is evident that further investigation, prototyping, and evaluation of communications security server options will be necessary.

6. ALTERNATIVE #4

Alternative #4 describes an enhanced services implementation. The next logical extension to Alternative #3 is to add local services and administration/management capabilities to the LAN. Servers are typically incorporated into a LAN to provide one or more of the following services: electronic mail, shared files, shared databases, and shared peripherals (i.e., printers, plotters, modems).

The MITRE LAD utilized a Novell server to provide these local services. The Novell server was configured to allow the sharing of files among local workstations. Although a Novell server is capable of providing additional services, the MITRE LAD documentation did not clearly identify how to take advantage of these services in a LAD environment.

Due to potential space constraints and fielding requirements, it is desirable that a single physical box be capable of simultaneously functioning as all of the required servers. Additionally, it would be extremely desirable for this box to also be able to function as the communications security server. The remainder of this alternative will be described in terms of a Unix server implementation. It should be understood that this alternative need not be restricted to a Unix implementation.

A Unix box with the proper software configuration is capable of functioning as a file server, mail server, print/plotter server and compute server. In addition to the software on the Unix box, each workstation will need to be configured with the corresponding client software.

Unix comes with a standard set of utilities which allow the basic administration and management functions to be performed. It is well known that these utilities are not designed for the novice. Thus, some recent releases of commercial versions of Unix are incorporating menu driven system administration tools. Although this sounds hopeful, a great deal of knowledge is still required to administer a full featured Unix implementation.

6.1 REQUIRED HARDWARE

In addition to the hardware required for the previous alternatives, this alternative requires a box capable of functioning as a Unix server. Any Intel 486 or

386 based workstation with sufficient RAM and hard disk to support the Unix implementation should suffice.

6.2 REQUIRED SOFTWARE.

The Unix server would require the following software:

a. Unix 'C2' operating system (BSD, or System V based)

b. Network File System Daemon (NFSD)

c. Line Printer Daemon (LPD)

d. Telnet Daemon.

e. File Transfer Protocol Daemon. (FTPD)

f. Unix SMTP based mail.

g. Optional Post Office Protocol Daemon (POPD)

h. Optional database server software.

Items "a" thru "f" above typically come bundled with the Unix implementation.

Every workstation will require the following software in addition to that previously described:

- NFS client for DOS

- Line Printer Request (LPR)

- Optional POP mail client for DOS

6.3 SECURITY FEATURES

The addition of a network file system will provide the ability to automatically store individual workstation audit entries on the file server. This is beneficial from a security prospective and also from an administrative point of view.

In general, the server operating system should provide a C2 level of security as described in the 'Orange Book'. All security relevant events should be audited.

6.4 ACCREDITATION ISSUES

The addition of local services should be implemented so that they do not hinder the ability to accredit the LAN for attachment to the DSNET3 packet switched node. It will be necessary to investigate the security of the various service implementations. For example, if the server requires the workstation to provide a password it is important that the password is not stored on the workstation in a manner which can be compromised.

6.5 FUNCTIONALITY.

In addition to the functionality described in previous alternatives, the following will be included:

a. Ability to construct mail messages from the workstation and deliver them locally or to locations across DSNET3.

b. Access to network hard drives and printers.

c. Centralized system administration/management functions.

6.6 ADVANTAGES

The major advantage of this configuration over those previously defined is the additional functionality provided by the network servers.

6.7 DISADVANTAGES

The additional functionality does not come without a price. There will be a requirement to perform additional administrative functions to maintain the services. The degree of difficulty imposed by this is based on the expertise of the system administer and the user-friendliness and intelligence built into the system administration utilities. It may be possible to build administrative shells around existing utilities in order to provide the appropriate level of user-friendliness.

An additional disadvantage of adding services to the LAN is the requirement for client software which must run on the workstation. The client software often requires a memory commitment from each of the workstations. The amount of memory required is based on the implementation. It is desirable to be able to dynamically load and unload the client software without re-booting the workstation.

6.8 TECHNICAL UNKNOWNS

In addition to the concerns identified in Section 5.8, the technical unknowns for this alternative center around the specifics of the implementation. For example, will the client software running on the workstation allow sufficient memory for other FAISS applications to be loaded?

Providing the mail, print, and file services with a Unix implementation is fairly straight forward. However, further investigation will be required to provide a user-friendly administration, management interface, and ensure server security requirements are met.

7. ALTERNATIVE #5

FORSCOM has contracted with GTRI under contract DAKF12-90-C-0020 for the purpose of advancing the current FAISS architecture to a more portable, open system based architecture with enhanced functionality. The project has been divided into two major efforts labeled Block I and Block II in accordance with the statement of work leading to the contract award. The goal of the Block I effort is to redesign the FAISS core software and to implement this redesign in a manner which lends itself to portability and openness. Under the Block II effort, networking and security considerations will be expanded to include research, evaluation, and prototyping components. A strong emphasis will be placed on conforming to emerging standards such as the US Government OSI Profile (GOSIP), the Portable Operating System Interface (POSIX), multi-level security requirements, and other applicable networking and computing standards.

The architecture and requirement specifics for this alternative will be identified through the Block II research effort.

8. SUMMARY

This document has provided a brief outline of alternative configurations for FAISS LAN connectivity to DODISS. The first two alternatives appear to be acceptable only as interim solutions where physical security procedures can compensate for weak system security. The addition of a communications security server overcomes the system security weakness, but does not provide LAN users with valuable services and administration tools. Network servers and utilities can be added to the LAN, but often require qualified personnel to maintain and operate them.

The long term multi-level security and connectivity requirements for the FAISS are being investigated by GTRI under the Block II effort of contract DAKF12-90-C-0020. The requirement for an intermediate FAISS LAN has not been identified by FORSCOM.

9. ACRONYM LIST

ACRONYM	MEANING
ALG	Application Level Gateways
ARPA	Advanced Research Projects Agency
BSD	Berkeley Software Distribution
CGA	Color Graphic Adapter
COTS	Commercial off the Shelf
DEC	Digital Equipment Corporation
DCA	Defense Communications Agency
DCN	Document Control Number
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DIAM	DIA Manual
DODIIS	Department of Defense Intelligence Information System
DSNET III	Defense Secure Network III
EGA	Enhanced Graphics Adapter
FAISS	FORSCOM Automated Intelligence Support System
FCA	Functional Configuration Audit
FCJ2	FORSCOM J2 (Directorate of Intelligence)
FORSCOM	Forces Command
FTP	File Transfer Protocol
GOSIP	Government OSI Profile
GTRI	Georgia Tech Research Institute
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPX	Internet Packet eXchange
LAN	Local Area Network
LAD	LAN Access to DODIIS
LPD	Line Printer Deamon
LSO	LAD Security Officer
MAC	Media Access Control
MLS	Multi-Level Secure
MX	Mail eXchange
MIB	Management Information Base
NFS	Network File System
NIC	Network Information Center
NVDET	Network Virtual Data Entry Terminal
OSI	Open Systems Interconnection
POPD	Post Office Protocol Deamon
POSIX	Portable Operating System Interface
PSN	Packet Switched Node

RIPSO	Revised IP Security Option
RFC	Request For Comments
RPC	Remote Procedure Call
SCI	Sensitive Compartmented Information
SA	Systems Administrator
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPX	Sequence Packet eXchange
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VGA	Video Graphics Array
WAN	Wide Area Network
XDR	eXternal Data Representation